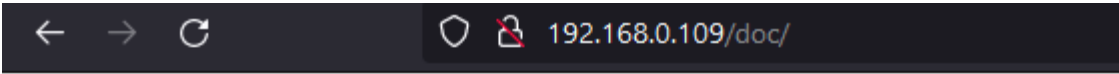


Domain: 192.168.0.109

Vulnerability Name	Directory listing vulnerability
Severity	5.3 - Medium
CVSS Score	Base Score: 5.3 Medium CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N
Description	A directory listing vulnerability occurs when a web server is configured to show the contents of a directory (i.e., a list of files and folders) when no default page (like index.html) is present. If the server is misconfigured and allows directory listing, it can expose sensitive information to potential attackers.
Attack Scenario	As an attacker, When we have scanned the target system for existing directories on the web root directory, we have identified that the directory “/doc/” on the server allows the attacker to list out the directory contents. Impact: Attackers can leverage directory listing vulnerabilities to gather information about the server's structure and potentially discover security holes. They may use this information to plan further attacks, such as exploiting known vulnerabilities in specific files or gaining unauthorized access to sensitive areas of the server.
Vulnerable Location	http://192.168.0.109/doc/
Vulnerable Parameters	Directory listing
Reproduction Steps	1. Access the below URL 2. URL: http://192.168.0.109/doc/ 3. Observe that directory contents listed out on the screen
Remediation	1. Don't allow users to access the directory “/doc/” instead display custom 403 page. 2. Don't allow users to access any directory on the server directly. 3. Don't allow directory listing.
Sample Code	N/A
Reference	Link1 Link2

Proof of concept:



Index of /doc

Name	Last modified	Size	Description
Parent Directory		-	
acl/	14-Nov-2007 05:59	-	
adduser/	16-Mar-2010 19:00	-	
ant/	23-Mar-2010 17:54	-	
antlr/	23-Mar-2010 17:54	-	
apache2-mpm-prefork/	16-Apr-2010 02:10	-	
apache2-utils/	30-Mar-2010 10:43	-	
apache2.2-common/	16-Apr-2010 02:10	-	